National Phase of PCT/EP99/09978 in U.S.A.
Title: Device and Method for Producing an Encoded Audio and/or Video Data Stream
Applicants: ALLAMANCHE; HERRE; KOLLER; RUMP

Translation of Amendments under Art. 34 PCT as attached to the IPER

For applications that do not require such maximum protection, the described concept is disadvantageously in that it can become relatively expensive and can require significant modifications to players in order to be able to process the determination data block. The players that are mass products in the consumer area after all, and therefore have to be offered inexpensively should, however, if possible, not having to be changed at all in order to be able to play protected pieces of multimedia. Thus, it has to be noted that the known encryption concept makes a maximum protection and high encryption flexibility possible by respectively designing the start block, but that, however, distinctive changes with the players are necessary in order to decrypt encrypted files or to read them at all.

U.S. Patent No. 5,796,838 discloses a method and an apparatus for carrying out an inversion of a frequency spectrum. The inversion of the frequency spectrum is achieved by converting a non-encrypted audio signal from analog to digital. The audio signal is then subjected to a positive complex frequency translation such that the negative frequency components of the audio signal will be positioned at around 0 Hz. The audio signal converted regarding to its frequency will then be low-pass filtered, so that only the base band components are left. The filtered complex base band signal will then be subjected to an arbitrary complex frequency displacement in order to position the signal frequency in a desired frequency band. The resulting signal has an inverted spectrum relative to the original audio signal. Extracting the real part of the complex samples will generate the final audio signal.

U.S. Patent No. 4,534,037 discloses a method and an apparatus for a scrambled pulse code modulation transmission or recording. In order to emphasise special spectral components of a sequence of digital signals that have been transmitted or recorded in pulse code words, "repacked" words are established comprising one or several

bits of a word of the original sequence and a complementary number of bits of the following word. The bits of a word out of which a "repacked" word consists of will be inverted prior to repacking such that, for example, the fourfold sampling frequency, the double sampling frequency or the sampling frequency itself can be emphasised in the spectrum. It is possible to transform the frequency spectrum downward regarding to the frequency without inversion of words.

It is the object of the present invention to provide a different concept for decrypting and encrypting audio and/or video signals, respectively.

This object is achieved by an apparatus for generating an encrypted data stream according to claims 1, 17 or 18 by an apparatus for generating a decrypted data stream according to claims 19 or 23, by a method for generating an encrypted data stream according to claim 29 and by a method for generating a decrypted data stream according to claim 30.

CLAIMS

1. Apparatus (10) for generating an encrypted data stream from an audio signal, comprising:

an encoder (16) for encoding the audio signal in order to generate a data stream with a predefined data stream syntax as output signal;

an encryption means (18) coupled with the encoder (16) for influencing encoder internal data (20a) in a uniquely reversible manner based on a key (k1) such that the generated encrypted data stream comprises payload information differing from payload information of a data stream that would be generated by the apparatus (10) without the presence of the encryption means (18) and that the generated encrypted data stream comprises the predefined data stream syntax,

wherein said encoder is an encoder for audio signals, comprising:

an analysis filter bank (204) for converting the audio signal from the time domain into a spectral representation in order to obtain spectral values;

a quantizing means (206) for quantizing the spectral values under consideration of a psychoacoustic model (208); and

an entropy encoder (210) arranged to carry out an entropy encoding of the quantized spectral values via a plurality of predefined code tables wherein each code table for the entropy encoding of quantized spectral values is provided in a frequency band and wherein at least one frequency

band comprises two or more quantized spectral values, and

wherein said encryption means (18) is arranged to resort the two or more quantized spectral values in the frequency band comprising two or more quantized spectral values having an associated code table based on the key.

2. Apparatus according to claim 1, wherein said encryption means (18) is further arranged to resort the two or more quantized spectral values in such a way that the encrypted data stream has the same length in bits as a data stream that would be generated by the apparatus (10) without the presence of the encryption means.

3. Apparatus according to one of the previous claims, wherein said encryption means (18) is arranged in order to resort the two or more quantized values based on the key merely in such a way that the payload information of the encrypted data stream differ only so strongly from the payload information of a data stream that would be generated without the presence of the encryption means (18), that a decoder that does not possess the key provides a decoded output signal based on the encrypted data with a quality that is lower than the quality that the decoder would provide if it possessed the key, wherein however, a minimum quality is ensured.

4. Apparatus according to claim 1 to 3, wherein the quantizing means (206) is arranged for generating the quantized spectral values as main information and scale factors as side information each of which is associated to at least one quantized spectral value; and

wherein said encryption means (18) is further arranged to influence the scale factors generated by said quantizing means (206) based on the key.

5. Apparatus according to claim 1, wherein said encryption means is arranged to link the quantized spectral values in the frequency band comprising two or more spectral values with a pseudo random bit sequence generated as start value based on the key via an EXCLUSIVE-OR-link.

6. Apparatus according to claim 1, wherein further merely least significant bits of spectral values are linked with a pseudo random bit sequence.

7. Apparatus according to claim 1, wherein said quantized spectral values are signed and wherein said encryption means (18) is further arranged to change the signs of quantized spectral values based on the key.

8. Apparatus according to claim 1, wherein said entropy encoder (210) is arranged such that it comprises at least one code table which is an unsigned code table such that a sign for a code word from the code table is written separately from the code word into the payload information, wherein said encryption means (18) is further arranged to change the sign of at least one quantized spectral value based on the key before said entropy encoding of said quantized spectral values.

9. Apparatus according to claim 1, wherein at least one code table of the plurality of code tables is a multidimensional code table, wherein a code word represents a plurality of quantized spectral values, wherein said encryption means (18) is arranged to resort groups of quantized spectral values, wherein one group of spectral values comprises so many

quantized spectral values as encoded by a code word of said multidimensional code table.

10. Apparatus according to one of the previous claims, wherein said encoder comprises a plurality of sub-blocks (204 to 210) connected with a bit stream multiplexer (212) multiplexing data output from the single sub-blocks according to the predefined data stream syntax in order to obtain the output data of said encoder (16).

11. Apparatus (70) for generating a data stream encrypted based on a second key (k2) from a first data stream encrypted based on a first key (k1), wherein said first data stream is an audio signal encoded by using an encoder with a predefined data stream syntax, wherein said first data stream is encrypted such that two or more quantized spectral values in a frequency band comprising two or more quantized spectral values and having an associated code table have been resorted based on the first key, wherein after the resorting an entropy encoding of the quantized spectral values has been carried out via a plurality of predefined code tables, wherein each code table is provided for the entropy encoding of quantized spectral values in a frequency band and wherein at least one frequency band comprises the two or more quantized spectral values, comprising:

a partial decoder (36') for reversing part of the encoding such that the resorted two or more spectral values are present;

a decryption means (38) for decrypting the resorted two or more spectral values by reversing the resorting based on the first key (k1);

an encryption means (18) for influencing the sequence of the two or more spectral values of the frequency band that has an associated code table based on the second key (k2);

a partial encoder (16') for carrying out part of the encoding that has been reversed by the partial decoder (36') in order to generate the data stream encrypted based on the second key (k2), wherein the second data stream has the predefined data stream syntax.

12. Apparatus (70') for generating a second data stream encrypted based on a key (k1) from a first data stream, wherein said first data stream is an audio signal encoded by using an encoder with a predefined data stream syntax, comprising:

a partial decoder (36') for reversing part of the encoding such that quantized spectral values of the audio signal are present;

an encryption means (18) for resorting two or more quantized spectral values in a frequency band comprising two or more spectral values based on the first key (k1), wherein one of a plurality of predefined code tables is associated to the frequency band for the entropy encoding, wherein each code table is provided for an entropy encoding of quantized spectral values in a frequency band and wherein at least one frequency band comprises the two or more quantized spectral values, wherein the encryption means is arranged to resort the quantized spectral values that have the same associated code table;

a partial encoder (16') for carrying out part of the encoding that has been reversed by the partial decoder (36') in order to generate the data stream encrypted

based on the key (k1), wherein the second data stream has the predefined data stream syntax.

13. Apparatus (80) for generating a decrypted data stream from a first data stream encrypted based on a key (k1), wherein said first data stream is an audio signal with a predefined data stream syntax encoded by using an encoder, wherein said first data stream is an audio signal with a predefined data syntax encoded by using an encoder wherein the first data stream is encrypted such that at least two or more quantized spectral values in a frequency band have been resorted based on the first key (k1), wherein a plurality of predefined code tables for an entropy encoding is associated with the frequency band whose quantized spectral values have been resorted, wherein each code table for the entropy encoding is provided for the entropy encoding of quantized spectral values in a frequency band and wherein at least one frequency band comprises the two or more quantized spectral values, comprising:

a partial decoder (36') for reversing part of the encoding such that the resorted two or more quantized spectral values are present, wherein the resorted two or more quantized spectral values belong to a frequency band that has an associated code table;

a decryption means (38) for decrypting the resorted two or more quantized spectral values by reversing the resorting based on the key (k1);

a partial encoder (16') for carrying out part of the encoding that has been reversed by the partial decoder (36') in order to generate the second data stream with the predefined data stream syntax.

14. Apparatus according to claims 11 to 13, wherein said partial decoder (36') comprises a bit stream demultiplexer (222), wherein said encoder internal data are the output data from the bit stream demultiplexer (222).

15. Apparatus according to claim 19, wherein said partial decoder (36') further comprises an entropy decoder (224) following the bit stream demultiplexer (222), wherein said encoder internal data are the output data from the entropy decoder (224).

16. Apparatus according to claim 17 to 19, wherein scale factors are influenced apart from the two or more quantized spectral values.

17. Apparatus (30) for generating a decrypted audio signal from an encrypted data stream comprising quantized spectral values of an audio signal being resorted and afterwards entropy encoded within a frequency band in a uniquely reversible manner, wherein the frequency band is defined that it has an associated code table from a plurality of code tables for the entropy encoding wherein the encrypted data stream comprises payload data differing from payload data of a non-encrypted data stream and wherein the encrypted data stream comprises the same data stream syntax as a non-encrypted data stream, comprising:

a decoder (36) for decoding input data in order to generate decoded output data, wherein the decoder comprises an entropy decoder (24) for reversing the entropy encoding in order to obtain the resorted quantized spectral values; and

a decryption means (38) for influencing the resorted quantized spectral values based on a key in order to reverse the uniquely reversible resorting that has

been carried out in an apparatus for generating an encrypted data stream in order to obtain the decrypted audio signal.

18. Apparatus (30) according to claim 17, wherein said decoder further comprises:

a plurality of functional blocks coupled with a bit stream demultiplexer (222) conducting parts of the data stream to the single blocks according to the predefined data stream syntax.

19. Apparatus (30) according to claim 18 or 19, wherein said decoder (36) further comprises:

a synthesis filter bank (228) in order to convert a spectral representation of the audio signal into a timely representation.

20. Method (70) for generating an encrypted data stream from an audio signal, comprising:

encoding (16) the audio signal in order to generate a data stream with a predefined data stream syntax as output signal;

encrypting encoder internal data (20a) by influencing the same in a uniquely reversible manner based on a key (k1) such that the generated encrypted data stream comprises payload information differing from payload information of a data stream that would be generated without the step of encrypting and that the generated encrypted data stream comprises the predefined data stream syntax,

wherein in the step of encoding an audio signal is encoded, comprising:

converting (204) the audio signal from the time domain into a spectral representation in order to obtain spectral values;

quantizing the spectral values under consideration of a psychoacoustic model (208); and

entropy encoding (210) of the spectral values via a plurality of predefined code tables wherein each code table for the entropy encoding of quantized spectral values is provided in a frequency band and wherein at least one frequency band comprises two or more quantized spectral values, and

wherein said step of encrypting (18) is carried out to resort the two or more quantized spectral values in the frequency band comprising two or more quantized spectral values having an associated code table based on the key.

21. Method (70) for generating a second data stream encrypted based on a second key (k2) from a first data stream encrypted based on a first key (k1), wherein said first data stream is an audio signal with a predefined data stream syntax encoded by using an encoder, wherein said first data stream is encrypted such that two or more quantized spectral values in a frequency band comprising two or more quantized spectral values and having an associated code table have been resorted based on the first key, wherein after the resorting an entropy encoding of the quantized spectral values has been carried out via a plurality of predefined code tables, wherein each code table is provided for the entropy encoding of quantized spectral values in a frequency band and

wherein at least one frequency band comprises the two or more quantized spectral values, comprising:

reversing (36') part of the encoding such that the resorted two or more spectral values are present;

decrypting (38) the resorted two or more spectral values by reversing the resorting based on the first key (k1);

encrypting (18) by influencing the sequence of the two or more spectral values of the frequency band that has an associated code table based on the second key (k2);

carrying out (16') the part of the encoding that has been reversed by the step of reversing (36') in order to generate the data stream encrypted based on the second key (k2), wherein the second data stream has the predefined data stream syntax.

22. Method (70') for generating a second data stream encrypted based on a key (k1) from a first data stream, wherein said first data stream is an audio signal with a predefined data stream syntax encoded by using an encoder, comprising:

reversing (36') part of the encoding such that quantized spectral values of the audio signal are present;

encrypting (18) by resorting two or more quantized spectral values in a frequency band comprising two or more spectral values based on the first key (k1), wherein one of a plurality of predefined code tables is associated to the frequency band for the entropy encoding, wherein each code table is provided for an entropy encoding of quantized spectral values in a frequency band and wherein at least one frequency band

comprises the two or more quantized spectral values, wherein the encryption means is arranged to resort the quantized spectral values that have the same associated code table;

carrying out (16') part of the encoding that has been reversed by the partial decoder (36') in order to generate the data stream encrypted based on the key (k1), wherein the second data stream has the predefined data stream syntax.

23. Method (80) for generating a decrypted data stream from a first data stream encrypted based on a key (k1), wherein said first data stream is an audio signal with a predefined data stream syntax encoded by using an encoder, wherein said first data stream is encrypted such that at least two or more quantized spectral values in a frequency band have been resorted based on the first key (k1), wherein a plurality of predefined code tables for an entropy encoding is associated with the frequency band whose quantized spectral values have been resorted, wherein each code table for the entropy encoding of quantized spectral values is provided in a frequency band and wherein at least one frequency band comprises the two or more quantized spectral values, comprising:

reversing (36') part of the encoding such that the resorted two or more quantized spectral values are present, wherein the resorted two or more quantized spectral values belong to the frequency band that has an associated code table;

decrypting (38) the resorted two or more quantized spectral values by reversing the resorting based on the key (k1);

carrying out (16') part of the encoding that has been reversed by the step of reversing (36') in order to generate the second data stream with the predefined data stream syntax.

24. Method (30) for generating a decrypted audio signal from an encrypted data stream comprising quantized spectral values of an audio signal being resorted and afterwards entropy encoded within a frequency band in a uniquely reversible manner, wherein the frequency band is defined by having an associated code table from a plurality of code tables for the entropy encoding wherein the encrypted data stream comprises payload data differing from payload data of a non-encrypted data stream and wherein the encrypted data stream comprises the same data stream syntax as a non-encrypted data stream, comprising:

decoding (36) input data in order to generate decoded output data, wherein in the step of decoding an entropy encoding (24) for reversing the entropy encoding is carried out in order to obtain the resorted quantized spectral values; and

decrypting (38) by influencing the resorted quantized spectral values based on a key in order to reverse the uniquely reversible resorting that has been carried out by generating an encrypted data stream in order to obtain the decrypted audio signal.

25. Apparatus (10) for generating an encrypted data stream from an audio signal, comprising:

an encoder (16) for encoding the audio signal in order to generate a data stream with a predefined data stream syntax as output signal;

an encryption means (18) coupled with the encoder (16) for influencing encoder internal data (20a) of the encoder (16) in a uniquely reversible manner based on a key (k1) such that the generated encrypted data stream comprises payload information differing from payload information of a data stream that would be generated by the apparatus (10) without the presence of the encryption means (18) and that the generated encrypted data stream comprises the predefined data stream syntax,

wherein said encoder is an encoder for audio signals, comprising:

an analysis filter bank (204) for converting the audio signal from the time domain into a spectral representation in order to obtain spectral values;

a quantizing means (206) for quantizing the spectral values under consideration of a psychoacoustic model (208); and

an entropy encoder (210) arranged to carry out an entropy encoding of the spectral values in order to obtain a sequence of code words wherein the sequence of code words represents an entropy encoded version of the audio signal, and

wherein said encryption means (18) is arranged to resort the sequence of code words by changing an order of code words based on the key.

26. Apparatus according to claim 25, wherein said encryption means (18) is arranged in order to resort the code words based on the key merely so strongly that the payload information of the encrypted data stream differs only so strongly from the payload

information of a data stream that would be generated without the presence of the encryption means (18) that a decoder that does not possess the key provides a decoded output signal based on the encrypted data with a quality that is lower than the quality that the decoder would provide if he possessed the key, wherein however, a minimum quality is ensured.

27. Apparatus according to claim 25 or 26, wherein always two adjacent code words are exchanged with each other.

28. Apparatus (70) for generating a data stream encrypted based on a second key (k2) from a first data stream encrypted based on a first key (k1), wherein said first data stream is an audio signal with a predefined data stream syntax encoded using an encoder, wherein said first data stream is encoded such that a sequence of code words generated by entropy encoding of quantized spectral values has been resorted by changing an order of code words based on the first key (k1), comprising:

a partial decoder (36') for reversing part of the encoding such that the resorted sequence of code words is present;

a decryption means (38) for reversing the resorting based on the first key (k1);

an encryption means (18) for resorting the sequence of code words based on the second key (k2) by changing an order of code words;

a partial encoder (16') for carrying out part of the encoding that has been reversed by the partial decoder (36') in order to generate the data stream encrypted based on the second key (k2), wherein the second data stream has the predefined data stream syntax.

29. Apparatus (70') for generating a second data stream encrypted based on a key (k1) from a first data stream, wherein said first data stream is an audio signal with a predefined data stream syntax encoded by using an encoder, comprising:

a partial decoder (36') for reversing part of the encoding such that a sequence of code words generated by entropy encoding of quantized spectral values is present;

an encryption means (18) for resorting the sequence of code words based on the key (k1) by changing an order of code words;

a partial encoder (16') for carrying out part of the encoding that has been reversed by the partial decoder (36') in order to generate the data stream encrypted based on the key (k1), wherein the second data stream has the predefined data stream syntax.

30. Apparatus (80) for generating a decrypted data stream from a first data stream encrypted based on a key (k1), wherein said first data stream is an audio signal with a predefined data stream syntax encoded by using an encoder, wherein said first data stream is encrypted such that a sequence of code words generated by entropy encoding of quantized spectral values has been resorted by changing an order of code words based on the first key (k1), comprising:

a partial decoder (36') for reversing part of the encoding such that the resorted sequence of code words is present;

a decryption means (38) for reversing the resorting of the sequence of code words based on the key (k1);

a partial encoder (16') for carrying out part of the encoding that has been reversed by the partial decoder (36') in order to generate the second data stream with the predefined data stream syntax.

31. Apparatus (30) for generating a decrypted audio signal from an encrypted data stream comprising a sequence of code words generated by entropy encoding of quantized spectral values resorted in a uniquely reversible manner by changing an order of the code words wherein the encrypted data stream comprises payload data differing from payload data of a non-encrypted data stream and wherein the encrypted data stream comprises the same data stream syntax as a non-encrypted data stream, comprising:

a decoder (36) for decoding input data in order to generate decoded output data; and

a decryption means (38) for influencing the resorted sequence of code words based on a key in order to reverse the resorting that has been carried out in an apparatus for generating an encrypted data stream in order to obtain the decrypted audio signal.

32. Method (70) for generating an encrypted data stream from an audio signal, comprising:

encoding (16) the audio signal in order to generate a data stream with a predefined data stream syntax as output signal;

encrypting (18) by influencing encoder internal data (20a) in the step of encoding (16) in a uniquely reversible manner based on a key (k1) such that the generated encrypted data stream comprises payload information differing from payload information of a

data stream that would be generated by the apparatus (10) without the presence of the encryption means (18) and that the generated encrypted data stream comprises the predefined data stream syntax,

wherein the step of encoding (16) comprises:

converting (204) the audio signal from the time domain into a spectral representation in order to obtain spectral values;

quantizing (206) the spectral values under consideration of a psychoacoustic model (208); and

entropy encoding (210) the spectral values in order to obtain a sequence of code words wherein the sequence of code words represents an entropy encoded version of the audio signal, and

wherein in said step of encrypting (18) based on the key the sequence of code words is resorted by changing an order of code words.

33. Method (70) for generating a data stream encrypted based on a second key (k2) from a first data stream encrypted based on a first key (k1), wherein said first data stream is an encoded audio signal with a predefined data stream syntax, wherein said first data stream is encrypted such that a sequence of code words generated by entropy encoding quantized spectral values has been resorted by changing an order of code words based on the first key (k1), comprising:

reversing (36') part of the encoding such that the resorted sequence of code words is present;

reversing (38) the resorting based on the first key (k1);

decrypting (18) by resorting the sequence of code words based on the second key (k2);

carrying out (16') part of the encoding that has been reversed in the step of reversing (36') in order to generate the data stream encrypted based on the second key (k2), wherein the second data stream has the predefined data stream syntax.

34. Method (70') for generating a second data stream encrypted based on a key (k1) from a first data stream, wherein said first data stream is an audio signal encoded using an encoder with a predefined data stream syntax, comprising:

reversing (36') part of the encoding such that a sequence of code words generated by entropy encoding of spectral values is present;

encrypting (18) by resorting the sequence of code words based on the key (k1) by changing an order of code words;

carrying out (16') part of the encoding that has been reversed by the step of reversing (36') in order to generate the data stream encrypted based on the key (k1), wherein said second data stream has the predefined data stream syntax.

35. Method (80) for generating a decrypted data stream from a first data stream encrypted based on a key (k1), wherein said first data stream is an encoded audio signal with a predefined data stream syntax, wherein said first data stream is encrypted such that a sequence of code words generated by entropy encoding

spectral values has been resorted based by changing an order of code words on a first key (k1), comprising:

reversing (36') part of the encoding such that the resorted sequence of code words is present;

decrypting (38) by reversing the resorting of the sequence of code words based on the key (k1);

carrying out (16') part of the encoding that has been reversed by the step of reversing (36') in order to generate the second data stream with the predefined data stream syntax.

36. Method (30) for generating a decrypted audio signal from an encrypted data stream comprising a sequence of code words generated by entropy encoding quantized spectral values resorted by changing an order of code words in a uniquely reversible way wherein the encrypted data stream comprises payload data differing from payload data of a non-encrypted data stream and wherein the encrypted data stream comprises the same data stream syntax as a non-encrypted data stream, comprising:

decoding (36) input data in order to generate decoded output data; and

decrypting (38) by influencing the resorted sequence of code words based on a key in order to reverse the resorting that has been carried out in generating an encrypted data stream in order to obtain the decrypted audio signal.